Smartphone and handheld security for mobile business.

Mobile computing: Opportunities and risk

By providing professionals with convenient mobile access to email, business applications, customer information and critical corporate data, businesses can become more productive, streamline business processes and enable better decision making. With the new ease of access to information comes a responsibility to protect the organization's data as well as the investment in mobile devices.

In many ways, security risks for mobile computing are similar to those for other computing platforms. There are the usual concerns of protecting data, authenticating users, and shielding against viruses and other malicious code. But because of their mobility and compact size, smartphones and handhelds present some additional challenges:

- Smartphones and handhelds are more easily lost or stolen than laptop or desktop computers.
- Users often treat smartphones and handhelds as personal devices and must be trained to consider the security risks when they use these devices to access corporate data and networks.
- Because smartphones and handhelds frequently connect wirelessly, robust wireless security becomes essential.

Fortunately, a wide selection of robust security solutions makes it easy to protect device data and mobile access to corporate networks. In fact, common security practices for Palm® smartphones and handhelds are more robust than what is typically used with laptops and desktops. For example, database encryption is a standard safety measure with mobile devices but not with laptops. Even if the device is stolen, the data cannot be read from the hard drive without the decryption key.

Strong security is multi-layered and must be woven into the very fabric of an organization. This paper examines some of the key issues in mobile security and discusses security solutions for Palm handhelds and smartphones.

Note: To prevent confusion, this paper distinguishes between *Palm® smartphones and handhelds* and the *Palm OS*. Palm, Inc, is a licensee of the Palm OS (known as Garnet and referred to in this paper as the Garnet OS), which has the ability to innovate on top of the Garnet OS and often does so to build seamless integrated functionality into its products. When features in this paper are native to the OS, they will be called out as part of the Garnet OS. When features are value added, either by Palm or by third parties, they will be so noted.

Contents

Know thy enemy: Security risks

When forming a security strategy for mobile devices, the first step is to analyze the potential risk factors. Based on the relevant risks for your organization and applications, form a security plan that effectively counters each risk. The major security threats with mobile devices are theft and loss, password cracking, data interception, malicious code and host intrusion.

Theft and loss

The same factors that make smartphones and handhelds attractive to mobile users- their portability and convenience - also make them easy to misplace. Despite a user's best efforts, a device may be stolen or lost. With proper security measures, corporate data will be protected even if the device falls into the wrong hands, and the user will be able to return to productivity quickly.

To prepare for the worst case, IT should implement the following precautions for every handheld and smartphone that contains corporate data:

- **Mandate authentication.** Power-on authentication protects device data and networks from unauthorized users. All Palm® smartphones and handhelds include strong, effective built-in password protection. In addition, administrators may want to install security applications that enforce the organization's authentication policies.
- **Encrypt sensitive data.** Any data that the enterprise wants to protect should be encrypted when not in use. Data should also be encrypted before it is transmitted. Effective encryption protects data from thieves and hackers.
- **Back up data regularly**. A recent backup minimizes user downtime and enables quick restoration of data, applications and configuration. With regular backups, user data and profiles can be easily restored.
- **Establish procedures for revoking access permissions.** If a device is lost or stolen, administrators must be ready to quickly remove access rights to all corporate resources. Centralized directories such as LDAP make revoking permissions quick and easy.

Password cracking

With the advent of automated password cracking tools, password cracking has received a great deal of publicity. The most common automated attack is a "dictionary attack," where a cracker launches a program that uses a dictionary or other directory to generate password after password until a match is successful. To thwart password compromises, follow these best practices:

1. **Limits on log-in attempts.** Configure the security application to limit the number of failed log-in attempts. This is the single best way to defeat dictionary attacks. The security application on Palm handhelds includes configurable password limits with the ability to erase selected data when the limit is exceeded.
2. **Change passwords regularly.** Periodic password changes can reduce the damage done by stolen passwords. Too frequent changes, however, can be irritating to users.
3. **Enforce password policies.** Ensure users select passwords with a minimum length and special characters unrelated to their user ID and that are not in a dictionary.
4. **Use password generators.** If users are allowed to generate their own passwords, they often choose easy-to-guess words. Some generators create pronounceable non-words to help users memorize their password. The downside of complex passwords is that users are more likely to write them down, so aim for strong passwords that can be memorized.

Despite the publicity surrounding automated cracking tools, social engineering continues to be the most common method of compromising passwords. By applying these best practices and training users to guard their passwords, mobile devices will be well-protected against password attacks.

Data interception

Today's smartphones and handhelds offer a variety of ways to access and transmit data, including wireline, infrared (IR), wireless LAN (Local Area Network) technology like Bluetooth and 802.11, and wireless WAN (Wide Area Network) connectivity. Wireless networks are particularly vulnerable to data interception since data is transmitted over the air, making it harder to enforce a physical boundary. In addition to accessing unencrypted data, an eavesdropper may be able to determine the identities of the communicating parties. Once an identity is obtained, the perpetrator can masquerade as a legitimate user and send false messages or access system resources. (This is often referred to as a "man-in-the-middle attack.")

By implementing sound security procedures such as authentication, data encryption and message integrity checking, corporations can safeguard their data and communications. We discuss network specific security technologies and products below in Protect Data across the Network.

Malicious code

Malicious code can take the form of viruses, worms, or Trojan horses. Infections are most commonly transmitted through email attachments and downloading untrusted applications. A messaging server that inspects attachments before sending them to the device plus an anti-virus program with up-to-date signature files are critical to protecting applications and data from infection. If users download files from untrusted sources, run virus scans whenever new files are downloaded. In the event data is corrupted, a recent backup can quickly restore the system to health.

Host intrusion

Intrusion typically refers to a hacker or cracker taking advantage of background services to break into your machine. Background services give hackers an entrance into your system. Preventing just such an event is why personal firewalls have become such a big business. By this definition, intrusion is not possible with today's Palm® devices. Why? Simply, the Garnet OS does not run application services in the background. Thus, Palm smartphones and handhelds today do not need a firewall. Currently, the only way for a hacker to put malicious code on your Palm handheld or smartphone is through beaming, synchronization or wireless downloads. These routes can and should be protected by authentication, antiviral software and security policies.

Intrusion detection is equally as critical as prevention. Logging and monitoring are powerful tools in intrusion detection. Server-based applications should incorporate logging and SNMP (Simple Network Management Protocol) support to provide a foundation for detection and response. When events are logged, normal usage patterns can be discerned by analyzing logs over time. Deviations from normal usage patterns may be a red flag. A management solution, such as Intellisync™ Mobile Suite, generates transaction logs of user activity. These logs can be loaded into the organization's monitoring system to automate analysis and alerts.

Foundations of smartphone and handheld security

As more and more mission-critical data is accessed with mobile devices, securing that information becomes a top priority for IT. The key to reducing the risks associated with mobile computing is establishing, communicating and enforcing strong corporate security policies. However, security threats and solutions seem to change continuously. What criteria can be used to choose security standards and policies with confidence?

Establish security policies

Sound corporate policies are the foundation for preventing costly security breaches. Convicted hacker Kevin Mitnik testified that social engineering was his primary method of gaining entry to corporate systems. In Mitnik's own words: "I was so successful in that line of attack that I rarely had to resort to a technical attack."

One of the best ways to counteract social engineering is to establish, communicate and enforce strong corporate policies. Before deploying devices to users, first train them on the organization's security policies and practices. Best practices for creating security policies include:

1. **Extend current security policies to mobile devices.** For example, if corporate desktops require an eight-character alphanumeric password, so should the handheld or smartphone. Every machine that stores or accesses corporate data is a point of vulnerability and should be protected. Also, consistent policies reduce both administration and user training time.
2. **Leverage existing infrastructure.** Existing infrastructure, such as user directories and monitoring systems, can be leveraged to reduce redundant systems and enforce security policies. Many mobile business solutions support LDAP (Lightweight Directory Access Protocol), Active Directory, RADIUS and other user directories. Server-based solutions should generate logs that can be analyzed by the corporate monitoring system. Using existing systems lowers total cost of ownership, reduces administrative overhead, and minimizes human error.
3. **Choose standards-based practices and solutions.** Open standards enable hardware and software from disparate manufacturers to work together. Industry, government and de facto standards provide vetted guidance (e.g. FIPS, Common Criteria, 802.1x)

Once corporate policies have been established, it is wise to continuously check and enforce your policies. Systems management solutions are a good way to automate policy enforcement. For example, systems management software can enforce security policies and ensure only authorized users can synchronize to the network. Palm Solution Providers, including Credant and Trust Digital, offer security and systems management solutions with useful features such as:

- Asset inventory
- Knowledge of who is synchronizing to your network
- Synchronization prevention if user authentication fails
- Synchronization prevention if the security application is not installed
- Distribution of software and configurations

To go a step further, if company policy calls for strong passwords, administrators can test whether users have set sufficiently strong passwords with tools like L0phtCrack test.

Some forward-thinking companies have a Chief Security Officer who determines security policies for the entire organization. More commonly, security experts are dispersed throughout the organization. For such organizations, it is helpful to convene these experts as needed to create corporate policies, share best practices, and select core systems.

When the corporation demonstrates that security is taken seriously, employees will also take it seriously. Security policies should be consistent, centrally administered, and enforced. Such policies simplify management and reduce error while ensuring that all parts of the organization are protected.

Protect data on the device

Power-on authentication

The purpose of authentication is to prove that a party is who he or she claims to be. The first level of authentication involves accessing the device itself. Authentication protects corporate data and network access in the event of theft. Desktop computers can be physically secured – they can be locked in an office and bolted to a desk. Because smartphones and handhelds are more difficult to secure physically, it is important that an unauthorized person will not be able to access it. Every device running the Garnet OS has built-in password protection. This simple yet effective application has no back doors and includes features such as automatic locking options and hints for forgotten passwords. To ensure privacy, the password is hashed using MD5 and only the hash value is stored.

Current Palm® handhelds include Security 5p, an enhanced security application that features:

- **Data Encryption.** Users have the choice of two 128-bit encryption algorithms: AES (Advanced Encryption Standard) or RSA Security's RC4. Users can choose to encrypt all data or only selected data.
- **FIPS- validated cryptography.** AES encryption services are provided by Palm's FIPS 140-2 validated Crypto Manager
- **Intrusion Protection.** The best way to guard against a dictionary attack is to limit the number of failed password attempts. With Security 5p, users can set a limit for password attempts, and then select an action to be taken when the limit is exceeded: delete all data or delete private records only.

Managed security solutions from Palm Solution Providers, such as Trust Digital, Credant and Good Technology, enable the IT group to enforce device security policies. The administrator can make password protection mandatory for the user and set policies such as length and type of password, frequency of password change and timeouts, as well as control encryption and application access. In addition, such applications protect against dictionary attacks with data-wipe functionality. Policies are persistent on the device and can only be changed by the designated administrator.

Data encryption

Encryption of data stored on the device is vital to protecting sensitive data. Managed security solutions allow the IT group to control what data must be encrypted and offer the option of protecting individual databases with an additional level of password protection. A variety of encryption algorithms are available including AES, TDES, and Blowfish.

Palm Solution Providers, such as Credant, Trust Digital and Good Technology offer a wide selection of applications for handheld and smartphone data encryption. Encryption functionality is typically combined with advanced password protection, application access control and other features. Since sensitive data can reside not only on the device but also on expansion cards, these solutions extend encryption to SD (Secure Digital) and MMC (MultiMedia Card) expansion cards.

Malicious code protection

To date, there have been no successful virus attacks on the Palm platform. Since viruses are platform specific, Garnet devices are not susceptible to the thousands of viruses developed for the Windows platform. But when it comes to security, it is best not to be complacent. Protection from malicious code begins with good anti-virus software. Best-in-class vendors such as Symantec and Computer Associates offer anti-virus applications for Garnet. Most applications offer wireless or wired signature file updates, automatic file scanning, virus alerts, and code repair and removal.

Backup and recovery

When the worst happens, proper backup and recovery procedures can restore users to productivity quickly. Containing the impact of a security breach is critical. If an employee's handheld or smartphone is lost or stolen, their accounts should immediately be disabled on all systems, the device isolated from the network and, if possible, a data wipe command should be sent.

To get the user back up and running, their data needs to be restored to another device. If backups are performed regularly, recent data can be quickly recovered. Data backups can be performed locally via a PC or Mac-based HotSync® operation, a wireless over-the-air (OTA) backup or recovery (by third party solutions) or Secure Digital Input/Output (SDIO) backup cards.

Management solutions from providers like Intellisync or iAnywhere help companies manage smartphones, handhelds, applications, and content from a central location. Today's mobile system management solutions often combine security and management features into one application that can integrate with an organization's existing management infrastructure.

With Intellisync Mobile Systems Management, administrators can deploy applications for use in the field; manage, exchange, and deliver content; capture and store hardware and software information; automatically track mobile devices and their health; and provide automated backup and restoration.

Afaria from iAnywhere enables web-based administrative control of key security and management functions. Afaria provides automatic backup and restoration of data, profiles and configurations. The security module provided centralized, policy-based control over passwords, device and storage card encryption, and both administrator-instigated and offline data deletion.

Protect data across the network

Device and server authentication

User authentication ensures that only authorized users can gain access to system resources. Corporate networks and servers should require users to authenticate with a username and a secret and/or unique identifier before access is granted. For valuable assets, multi-factor authentication is often employed. The first factor is typically something a user knows (like a PIN or passphrase), and the second factor may be something a user has (such as a hardware or software token, certificate or smartcard). Biometric authentication (something the user is, such as a fingerprint or iris pattern) can be used alone or in combination with the other authentication mechanisms.

Server authentication should be used in transactions where the user is providing sensitive information such as a credit card number. To prove its identity, a server could use protocols such as Secure Socket Layer (SSL) or Secure Electronic Transaction (SET) to send a digital certificate, signed by a Certificate Authority, to the user.

The Garnet OS ROM includes root certificates for every major certificate authority. When establishing an SSL connection, the Garnet OS HTTP library uses these root certificates to authenticate the remote web server. Some large organizations act as certificate authorities and issue their own certificates to identify their secure web servers. Before a user can negotiate an SSL connection with the organization's servers, the self-issued root certificate must be added to the set of trusted root certificates in the user's browser. Palm developers can design the calling application to check the remote server's certificates and display a UI to add them as trusted.

The Garnet OS also has built-in Point-to-Point-Protocol (PPP) support using popular authentication protocols including the Challenge-Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), and Password Authentication Protocol (PAP). Palm® smartphones and handhelds also have multiple methods of unique device identification, including Hardware Serial Number (HSN), International Mobile Equipment Identity (IMEA), Electronic Serial Number (ESN) and Flash ID. Any of these unique identifiers can be used to authenticate the device for network access, allowing Palm smartphones and handhelds to be used as a physical token for two-factor authentication. Popular authentication tokens, such as RSA SecurID, can be used for two- or three-factor authentication. Up to eight RSA SecurID tokens can be stored on a Palm device, eliminating the need to carry multiple key fobs.

Communications encryption

End-to-end communications encryption ensures that even if data is intercepted, it will be useless to the interceptor. There are two general categories of encryption algorithms: symmetric key encryption and asymmetric (or public) key encryption. Symmetric encryption uses the same key for both encryption and decryption. Asymmetric encryption uses two keys, one public and one private.

With mobile devices, it is important to employ an efficient encryption algorithm that protects data without degrading performance or battery life. For example, AES (Advanced Encryption Standard) and DES (Data Encryption Standard) are faster and use less battery life than 3DES (Triple DES or T-DES).

The intended application also influences encryption algorithm and method selection. Symmetric key cryptography requires less computational overhead, so data can be encoded and decoded quickly. Symmetric encryption works well for encrypting data on the device since the encryption key never leaves the device. Public key cryptography is typically used to establish communication between two parties. In many applications, these methods are complementary. For example, wireless messaging may use asymmetric keys to establish a session between a client and server, and then use symmetric keys to encrypt the data that is exchanged.

The latest Garnet OS provides features such as expanded support for wireless communications and a suite of robust security options. The FIPS-validated Crypto Provider Manager (CPM) available in the Garnet OS provides encryption and security services. This cryptographic interface can support multiple encryption modules and has built-in algorithms including RC4 symmetric encryption, SHA-1 for hashing and RSA Verify for signature verification. The CPM was co-developed with RSA Security.

In addition, there are many cryptographic toolkits, Public Key Infrastructure (PKI) toolkits and cryptographic libraries available from leading security companies and open source code. A sampling of such toolkits is listed in the Appendix.

Secure administration

As mobile devices become more powerful and feature-rich, solutions to administer, secure and support these devices have become more robust. Solution Providers such as Trust Digital, Credant, Avocent, and Good Technology give administrators powerful tools to manage mobile devices from policy administration and device detection to monitoring and real-time control.

Trust Digital Trusted Mobility Server allows administrators to centrally manage the handhelds, smartphones, and wireless devices that connect to the organization's network. Administrators can apply profiles to specific groups and check for security setting conflicts, and push security policies to all mobile devices in the field. Mobile Asset Manager tracks devices software inventory and scans for system information such as OS, memory, disk space, display, and licensing.

Good Technology's GoodLink allows for secure over-the-air management of device software, policies, and settings. The Good Monitoring Portal provides a real-time view of the server and all users by device, carrier, software version, and coverage, so IT can quickly troubleshoot issues and minimize help desk costs. In addition, administrators can manage passwords remotely, distribute and manage security policy updates and change access permission, all over-the-air. For example, if a CFO loses his Treo™ smartphone, he can call IT to immediately erase all sensitive data and lock down the device.

Credant Mobile Guardian (CMG) detects and controls rogue mobile devices. CMG allows administrators to track the number and type of devices connecting to their network. It also gathers inventory information such as host name, IP address, device type, and OS version, as well as device statistics such as memory and battery life. To assist the help desk, CMG features self-service password reset and administrator-assisted access recovery. CMG also enforces security policies with three administrative modes to protect the network from unauthorized mobile devices:

- *Report Only* mode reports the details of a mobile device synchronization on the network, while still allowing the user to synchronize to their PC.
- *Report and Disable* mode blocks PC synchronization and reports the attempted synchronization to the CMG administrator.
- *Auto Install* mode installs CMG security software on any non-secured mobile device that attempts to synchronize on a networked PC. After the initial CMG software installation, subsequent policy updates are automatically pushed to the device.

PointSec includes a remote help feature that allows user to call their helpdesk to re-set their password and regain access to their encrypted information using a secure challenge/response procedure.

Avocent SonicSentinel allows administrators to monitor, secure and support wireless mobile devices in real-time. Features include:

- Real-time control of mobile devices
- Remotely lock down or hard reset a lost or stolen device
- Remotely erase selected data such as email, contacts or memory cards
- View real-time device statistics such as connectivity and installed software
- Receive alerts when a device has been offline for a defined period of time
- Enforce password policies by locking devices or configuring pop-up reminders to appear until users set up passwords

Avocent SonicAdmin allows administrators to securely connect to their network, diagnose problems, and fix them in real time from a Treo™ smartphone. Remote management is secured with a point-to-point, multi-layer security model that includes 3DES encryption, SSH and NTML authentication and optional SecurID authentication. An audit log records all administrative activity. Administrators can use Telnet or SSH to manage Unix and Linux servers as well as Telnet or SSH capable network equipment such as routers, switches, hubs, and printers. SonicAdmin includes mobile management of select enterprise applications including Microsoft Exchange and Lotus Domino Management.

Secure development

The latest Garnet OS Developer Suite is designed to help developers produce enterprise-grade applications. The Garnet OS Developer Suite is based on the industry-standard Eclipse environment, an open-source, Integrated Development Environment (IDE) originally developed by IBM that supports software development in a variety of languages, including C, C++, Java and COBOL. In addition, a wide variety of development tools are available for Garnet OS, including Metrowerks CodeWarrior, the Eclipse environment, Borland's tool suite and Microsoft .NET compatible tools from AppForge.

Securing HotSync and ports

Some high-security environments demand an additional level of security for the use of popular handheld and smartphone features such as Infrared, wireless connectivity, and cameras. Although users can disable Infrared and wireless radios via Palm Preferences, some agencies require administrative control of these settings.

Synchronizing data also comes under scrutiny, with the need to ensure that sensitive device data cannot be downloaded to an unauthorized workstation. There are several strong software solutions available to provide organizations with control over synchronization and hardware features in their Palm® devices.

Several Palm Solution providers, including Credant, Trust Digital and Motion Apps, allow administrators to control HotSync, port and peripheral functionality. For example, Credant Mobile Guardian provides automatic, transparent mutual authentication between the mobile device and the companion PC, protecting device data from being synchronized to a non-authorized workstation. Mobile Guardian also enables administrative control of infrared port, Bluetooth, camera and microphone functions, external storage access and network connectivity. Motion Apps mCamLock can disable the Treo 650 smartphone camera.

Network security solutions

Smartphones and handhelds can send and receive data using either wireline communications (via synchronization cradle) or wireless communications. Since cradle synchronization is inherently private, this discussion focuses on the privacy of wireless communications.

Palm® smartphones and handhelds support a variety of connectivity options, from WANs to WLANs (Wireless LAN) and PANs (Personal Area Networks). In addition, every Palm handheld and smartphone has a built-in IR port that allows simple, fast data transfer.

VPN

A VPN (Virtual Private Network) is a popular solution for securing access to intranet and extranet resources and data. Properly implemented, a VPN provides user authentication, encryption, and access control. VPN technology is in wide use today for laptops and workstations, enabling mobile deployments to leverage existing infrastructure.

An IPSec (Internet Protocol Security) VPN client is the most popular business-class VPN solution today. Internet Protocol Security (IPSec) VPN offers strong security with a selection of encryption and authentication options, as well as message authentication and integrity controls, allowing an organization to choose the level of security that balances requirements for privacy and performance. anthaVPN (formerly movianVPN) features extended authentication (XAUTH) support and works with many popular gateways, including Cisco, Lucent and Nortel.

Point-to-Point-Tunneling-Protocal (PPTP) VPN clients, such as Mergic VPN, are often used in small to mid-sized businesses. PPTP VPNs are easy to configure and are supported by most Cisco and Nortel gateways, as well as many Microsoft and Linux servers.

VPN technology is a great choice for organizations that utilize a variety of networks. Most VPN clients work over a virtually any network, including Ethernet LANs, GSM/GPRS, 1xRTT, 802.11, Bluetooth, IrDA and CDMA.

SSL

SSL (Secure Sockets Layer) is a popular transport security standard used in virtually every web browser on the market today. Wireless-capable Palm smartphones and handhelds include a built-in web browser that features SSL 2.0, SSL 3.0, and 128-bit encryption.

"SSL VPNs" are a fairly recent category that challenges traditional IPSec VPNs. SSL VPNs take advantage of the SSL built into virtually all web browsers to authenticate and encrypt transmitted data. The big advantage of many SSL VPNs is that no additional client software is needed other than a standard web browser. Once a backend SSL server is in place, information is transmitted securely using the browser software already included on all Palm smartphones and most handhelds. Another advantage is that this technology can be used over virtually any network. One current limitation is that only browser-based applications can be secured using an SSL VPN without additional client software.

802.11 Security

802.11 is a widely deployed and immensely popular WLAN technology. 802.11 security has received negative publicity due to vulnerabilities in the Wired Equivalent Privacy (WEP) standard. To correct WEP vulnerabilities, IEEE first ratified 802.1x, an interim standard that strengthened WEP authentication, and then issued 802.11i, the final standard for Wi-Fi security.

WPA substantially improves upon WEP security by using 802.1x authentication, Temporary Key Integrity Protocol (TKIP) encryption and message integrity checks. WPA2 is the Wi-Fi Alliance approved implementation of 802.11i. The main difference between WPA and WPA2 is WPA2's use of AES for data encryption. While the upgrade from WEP to WPA security only required a software upgrade in most cases, the upgrade to WPA2 typically requires a hardware upgrade or replacement.

The good news is that WPA2 is backward compatible with WPA. Since WPA offers strong security and WPA2 often requires a hardware replacement, many organizations wait until new equipment is needed to upgrade to WPA2.

802.1x and LEAP

For 802.11 LANs, a security solution based on the IEEE 802.1x standard is an excellent option. 802.1x uses EAP (Extensible Authentication Protocol) to authenticate between a wireless device and an access point before a device can access the WLAN. In addition, 802.1x uses automatic key rotation to solve WEP's much publicized key reuse issue. The most popular EAP types are LEAP, PEAP, TLS, and TTLS.

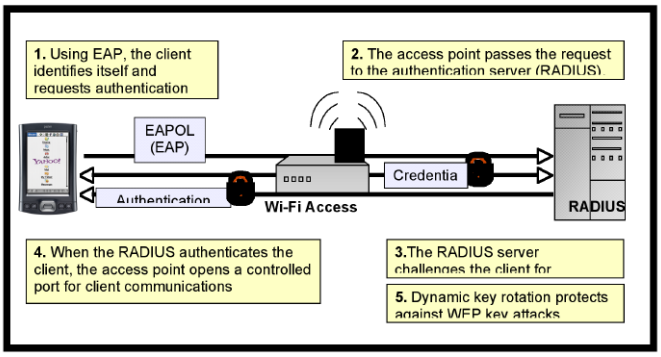

Diagram A: 802.1x (EAP-LEAP) Security

Cisco's LEAP (Lightweight EAP), based on the 802.1x standard, enforces mutual authentication between the client and access point. LEAP also addresses the WEP key reuse weakness by exchanging dynamic WEP keys. The "Lightweight" in LEAP refers to the processing usage, not the level of security, making LEAP particularly well suited to mobile devices. LEAP is quickly becoming a de facto standard. It addresses the security vulnerabilities of WEP and, due to Cisco's dominance as a Wi-Fi equipment manufacturer, has a significant user base.

Because LEAP relies on password authentication, LEAP's one known vulnerability is dictionary attack. This vulnerability can be effectively countered by limiting failed password attempts at the server. With Cisco Aironet access points, each user is given a unique session key. Furthermore, LEAP encrypts the broadcast WEP key with the session key before transmission.

Palm® devices with built-in Wi-Fi include WPA-PSK (Pre-Shared Key), also known as WPA Personal. WPA-PSK provides strong security without the need for a server or additional software.

802.11 and VPN

VPN is a weightier option for 802.11 security than 802.1x, both in terms of security measures and performance. Consider a VPN if your users need to transmit information over multiple networks, such as a WAN and a WLAN. One of the big advantages of VPN is that it will work over a variety of networks, including 802.11, GSM/GPRS, CDMA, Ethernet and Bluetooth. VPN is a good choice if an organization is already maintaining a VPN infrastructure and wishes to streamline the number of supported technologies.

In addition, many enterprise applications provide encryption and authentication as part of the base product. When building custom applications, organizations should consider incorporating encryption modules to protect data privacy during transmission.

Bluetooth® wireless technology security

Bluetooth is a PAN technology that wirelessly links devices within close proximity to one another (about 30 feet). Bluetooth enables spontaneous, or "ad-hoc" networks and requires no infrastructure.

While the Bluetooth specification does a respectable job of stipulating security features, potential security risks include man-in-the-middle attacks, as well as the possibility that other devices could access data by masquerading as connection-accepting or connection-seeking devices on the Bluetooth network. The Bluetooth protocol incorporates features to protect communications against these types of attacks, including:

- Mandatory user authorization before data transmission.
- Encryption based on the SAFER+ algorithm.
- New encryption keys for each session.
- Separate encryption keys for authentication and encryption.
- Frequency hopping algorithm to prevent interception of Bluetooth traffic.

All Bluetooth-capable Palm handhelds use link level security with 128-bit encryption to protect privacy and prevent over the air attacks. Bluetooth connections are authenticated through passkey exchange. Users can designate devices as "trusted" by exchanging passkeys. In addition, Bluetooth-capable Palm handhelds have a "Discoverable" setting, allowing users to hide their device from detection by another device doing an inquiry. For more information about Bluetooth on Palm handhelds and smartphones, please see the Palm Bluetooth white paper at www.palm.com/us/wireless/bluetooth

Additional security solutions can be used with Bluetooth devices to achieve enterprise-grade security. Many VPN clients run over Bluetooth, including anthaVPN and Mergic VPN. Alternately, PKI can be used to add strong authentication, encryption, digital signing and non-repudiation.

Infrared (IR) security

The IR port is a relatively secure means of communication. Palm devices must be in close physical proximity (4 feet or less) to beam successfully. The recipient is prompted when a beam is sent and must tap on the screen to accept incoming data. This allows the user to control what he or she receives. Palm handhelds also have built-in "sleep" thresholds (typically 1-3 minutes), and when sleeping the handheld cannot accept an incoming infrared beam. For organizations that need to deactivate the beaming feature, solutions from Credant, Trust Digital and others enable administrators to disable the IR port.

Secure messaging and data solutions

One of the great benefits of Palm smartphones and handhelds is the ability to access email, calendar, contacts and other important data almost anywhere. Organizations can equip mobile users with all the most popular mail servers, such as Microsoft Exchange/Outlook, Lotus Domino/Notes , Novel Groupwise, and POP or IMAP servers, in some cases directly to the server, and in others through third party middleware solutions such a GoodLink, RIM Blackberry Enterprise Server (in early 2006), Intelisync, and more.

Good Technology GoodLink Enterprise Edition

With Good Technology's GoodLink Enterprise Edition, users can exchange messages, access data in real-time, and manage phone calls from their Treo™ smartphone. GoodLink delivers a laptop-like experience, with full Microsoft™ Outlook capabilities, rich attachment support, multi-tasking and interaction with third party applications. GoodLink goes beyond Outlook to provide sync and browser access to BTFW (behind the firewall) databases and enterprise applications. Cradle-free synchronization allows continuous two-way wireless sync of Microsoft Exchange/Outlook (and Lotus Notes in 2006).

In March 2004, GoodLink was awarded FIPS140-2 validation on the Palm Treo. GoodLink's layered security protects communications between the server and the mobile device.

Client Security	• Authentication: Security policies such as password expiration, length, and format can be enforced. This functionality is integrated with the Garnet OS security application. Devices are authenticated with BTFW applications using unique and rotating certificates. • Remote data deletion: If a device is lost or stolen, the administrator can remotely delete sensitive data. • Backup: An SD "recovery card" stores a duplicate image of the device configuration and data for quick data recovery.
Transport Security	• Encryption: 192-bit AES is used to encrypt messages from GoodLink Server to the device. • Message confirmation: Positive confirmation architecture ensures messages have been delivered and provides persistent message storage and re-delivery.
Server Security	• BTFW server: GoodLink Server is installed behind the corporate firewall and uses standard port 443 to create an outbound initiated connection with the Good Security Operations Center. Good requires no open firewall ports or components that need to be deployed in a DMZ. • Role-based administration: IT can restrict security-related administration to a subset of administrators.

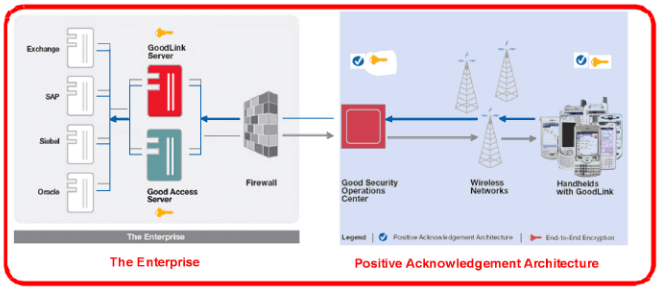

Diagram B: Security from GoodLinkServer to Treo smartphone

Government solutions

Smartphones and handhelds allow field personnel to quickly access mission critical information and communicate effectively with colleagues. As government agencies become more mobile, demand is growing for secure, wireless solutions that ensure communication continuity, increase productivity and reduce IT costs.

Federal standards

In the United States, NIST (National Institute of Standards and Technology) develops standards and guidelines for federal computer systems, which are issued as Federal Information Processing Standards (FIPS). Many U.S. federal agencies are required to use FIPS-validated technology, and many private-sector businesses regard FIPS validation as evidence of high quality security.

Palm's Crypto Manager is FIPS 140-2 validated. Crypto Manager can be used to provide strong cryptographic services to Garnet OS applications, ensuring that critical security functions such as encryption, decryption, key generation, checksums, and pseudo random number generation are performed correctly. For Crypto Manager's FIPS validation information, see Certificate #322 at http://csrc.nist.gov/cryptval/140-1/1401val2003.htm

HIPAA (Health Insurance Portability and Accountability Act) sets standards for healthcare plans, clearinghouses and providers that handle protected health information. The safeguards that comprise HIPAA's Final Security Rule focus on protecting "data integrity, confidentiality and availability" of individually identifiable health information. The many strong security solutions for Palm® smartphones and handhelds enable healthcare entities to implement HIPAA-compliant mobile solutions. For more information on making mobile devices conform to HIPAA, see Achieving HIPAA-Compliance with Palm handheld and smartphone solutions at http://www.palm.com/us/pdfs/hippa_wp.pdf

FIPS solutions for Palm handhelds and smartphones

A growing number of FIPS validated solutions are available for Palm smartphones and handhelds, giving government agencies a choice when it comes to deploying secure mobile solutions. FIPS 140 validation is designed specially for cryptographic modules. Often, these cryptographic modules are used as part of a larger security solution to ensure encryption, key creation, code signing, and other cryptographic functions are performed to FIPS standards.

There are three basic claims that vendors make in regard to FIPS: validated, compliant, or pending validation. FIPS validated solutions have successfully completed NIST's validation process and are listed on the NIST website. FIPS compliant solutions have not been validated or submitted for validation. Vendors simply are claiming that their solution has been built in compliance with published FIPS standards. FIPS validation pending means that vendors have completed the work of designing and building a solution to FIPS standards and have submitted their software to NIST for validation.

NIST typically takes 6-12 months to complete the validation process once a module has been submitted. During this waiting period, vendors often market their products as "FIPS validation pending." For the latest product-specific information about FIPS 140 status, please see the following NIST websites:

- For pre-validation status: http://csrc.nist.gov/cryptval/140PreVal.pdf
- For completed validations: http://csrc.nist.gov/cryptval/140-1/1401val.htm

FIPS solutions for Palm® smartphones and handhelds

PRODUCT	FEATURES
Cryptographic Libraries	
Certicom Security Builder GSE	Security Builder GSE enables developers to incorporate a complete FIPS 140-2 validated cryptographic module or individual FIPS-approved algorithms into applications.
CREDANT Mobile Guardian	Mobile Guardian is FIPS validated and uses FIPS-validated encryption algorithms, including AES, Triple-DES and SHA-1.
RSA Security BSAFE	BSAFE incorporates FIPS 140-validated cryptography for government applications that require this certification.
Palm Crypto Manager	Using the FIPS 140-2 validated Crypto Manager API, developers can access strong cryptographic services, including AES encryption, HMAC SHA-1 message authentication and SHA-1 digests.
PalmSource Cryptographic Provider Manager	This FIPS 140-2 validated cryptographic provider offers a broad variety of algorithms to Garnet OS developers, including AES, 3DES, SHA-1 and HMAC-SHA-1.
Trust Digital Mobile Edition	Mobile Edition, which is FIPS 140-2 validated, implements and enforces mobile security policies across multiple platforms.
Groupware and Data Access	
AppForge Data Sync	Data Sync also offers flexible user authentication, client database support and encryption options. Encryption options include FIPS 140-2 validated Triple DES, FIPS 140-2 validated AES, SSL and Certicom SSL Plus EE.
Good Technology GoodLink	The Good System's cryptographic module, with AES, TDES, SHA-1 and HMAC-SHA1 algorithms, has received FIPS 140-2 validation.
Extended Systems OneBridge Mobile Groupware	OneBridge Mobile uses a FIPS 140-2 compliant encryption module to secure data from the client to the server.
iAnywhere Pylon Anywhere	This mobile email and synchronization solution encrypts data between the Pylon Anywhere server and the device using AES, Triple DES or SSL. AES and Triple DES encryption are FIPS 140-2 compliant. Users can be authenticated against LDAP, Active Directory, Domino and NT Domains.
Intellisync Mobile Suite	FIPS 140-2 validated Mobile Suite offers wireless access to corporate and personal e-mail, calendar, contacts and other corporate data. Transmissions are secured end-to-end with AES and 3DES encryption.
Visto Mobile	Visto Mobile, a carrier-grade platform for wireless access to corporate and personal e-mail, calendar, contacts and other corporate data, is FIPS 140-compliant and offers end-to-end AES encryption.

Case study: FIPS Security in Action

Joel Yarmon, Technology Director of the Senate Committee on Commerce, Science and Transportation, needed to simplify support for his department's fleet of mobile devices. Too many versions of device and desktop software in addition to carrier issues made troubleshooting time-consuming and complex.

After evaluating many mobile devices and groupware solutions, he decided to deploy GoodLink Enterprise Edition and Treo™ smartphones. Immediately, Joel and his team found that their support burden decreased significantly. According to Joel, "GoodLink and Treo solution took the desktop out of the equation, making it very easy to diagnose problems." Furthermore, deploying a new Treo smartphone took only two minutes using an SD card or over-the-air provisioning. With GoodLink and Treo smartphones, Joel's team could restore users to working order from anywhere using wireless connectivity.

GoodLink's FIPS 140-2 validation is a requirement for sensitive Senate communications. With GoodLink and Treo smartphones, Senate users achieve the "continuity of work" that is critical to the government, particularly in a post-9/11 world. With GoodLink, IT can remotely erase a Treo smartphone if the device is lost or stolen. The device will send back a confirmation that the data has been wiped. In addition, all devices employ password protection that activates at power-on and after a short period of disuse.

"Since Treo is software running on software, it can do much more than just send email and make calls," Joel explains. With the Treo smartphone's speakerphone, SD card slot, stylus, Bluetooth, and broad network of software developers, the Senator and his staff can surf the Internet, manage all of their Outlook features, and tap into a wide selection of applications. Since GoodLink supports Garnet OS and Pocket PC platforms, users are free to choose their favorite mobile device. Joel notes that most users choose the Treo 650 smartphone, drawn to the wide range of applications, convenient form factor, sharp screen, one-handed operation and easy-to-use keyboard. And he observed, "The Treo smartphone offers more functionality than a BlackBerry device." The IT staff also appreciates that Palm is actively releasing firmware updates for Treo smartphones and providing up-to-date features and support that they need.

The future of smartphone and handheld security

Security has become a top priority for business, government and healthcare providers and many exciting developments are expected in the not-too-distant future. Security advances, such as biometric security and smartcard technology, will make strong mobile security easier to use and administrate.

Biometric systems analyze unique physiological traits such as fingerprints, hands, voices and facial patterns. What makes biometric systems so effective is that physical characteristics such as these are unique and very difficult to counterfeit. Voiceprint matching, fingerprint recognition, facial and hand geometry patterning, iris scanning and thermal detection are all possibilities for mobile device security. The beauty of biometric authentication is that it merges strength with convenience. Users can gain access simply by uttering a passphrase, touching a screen or scrawling their signature.

Smartcards contain integrated circuits that provide tamper-proof storage of user and account identity and protect against a full range of security threats, from careless storage of user passwords to sophisticated system hacks. Smartcards can work with Palm® smartphones and handhelds via the expansion slot, SIM card or a USB attachment. Potential applications include digital signing, strong authentication, and secure payment solutions.

The Common Access Card (CAC), a smartcard issued to US DOD (Department of Defense) employees, shows the principals of physical security, PKI and (soon) biometrics in action. The first generation of the CAC was used for system and building access and incorporated a digital certificate for signing email and documents. The plan for the second generation of cards is to incorporate biometrics, such as fingerprint and iris recognition, to further increase security and convenience. This solution could be extended to Palm devices by using an SD-or MMC-based smartcard as the CAC.

Biometrics and smartcards are just two examples of the new trend towards uniting convenience and strength in security technologies. By combining the expansion capabilities of Palm devices with new developments in the security industry, organizations can secure their data without compromising usability.

Conclusion

Today, smartphones and handhelds have evolved into indispensable business tools that enable an increasingly mobile workforce to remain connected and productive. As mobile devices proliferate and become an integral part of the corporate technology infrastructure, security becomes a serious concern for every IT manager as well as for users. Protecting corporate information is essential to business survival and growth, and end-users must be trained to safeguard these resources.

A clear understanding of the challenges posed by smartphones and handhelds in a particular environment provides the basis for developing sound security policies, standards and practices. A security strategy must strike a balance between what is possible and what is feasible, basing decisions on industry best practices and clearly articulating guidelines and procedures. Encryption programs, anti-virus software, effective password use, training and awareness are all components of an effective business security program. Palm and its Solution Providers are committed to developing products and solutions that enable organizations to adopt security best practices and minimize the risks involved in mobilizing their workforce.

Appendix: Solutions from Palm solution providers

Authentication and encryption solutions

PRODUCT	FEATURES
Biometric Solutions FobLock	Using fingerprint recognition, FobLock controls access to Palm® and other IrDA-enabled devices. FobLock can be used with its own or customized to work with an organization's database. www.biometricsolutions.com
Good Technology GoodLink Mobile Defense	GoodLink Mobile Defense provides enhanced password protection, data encryption and hardware button password entry. IT managers can enforce password, encryption and beaming policies and set restrictions on application usage. (Mobile Defense was formerly JP Mobile Surewave Mobile Defense) www.good.com
Mobile Armor Data Armor	Mobile Armor supplies mandatory authentication and encryption services to mobile devices. www.mobilearmor.com
Palm Security 5p	Included with most Palm handhelds, this security application features 128-bit FIPS-validated AES encryption, the ability to encrypt all or only selected databases, and dictionary attack protection www.palm.com
PointSec	Pointsec offers centralized managed security policies, including enforceable access control, account lockout, and authenticated HotSync. A challenge/response procedure helps users reset their password with minimal help desk intervention. www.pointsec.com
RSA Security SecurID	SecurID software, used in conjunction with RSA ACE/Server software, generates a random, one-time-use access code that automatically changes every 60 seconds. www.rsasecurity.com
SafeBoot Device Encryption	SafeBoot enables administrators to control multi-factor authentication, device and removable media encryption, if a device can synchronize with only the PC from which it was installed, and more. Centralized management includes rollout and deployment, audit, hot revocation, remote updates, and policy enforcement. www.safeboot.com
TealPoint Software TealLock	Corporate TealLock is a secure automatic locking program. Features include serial and infrared lockout, data encryption, administrator password, remote-unlocking, and password controls. www.tealpoint.com

Management & security solutions

PRODUCT	FEATURES
CREDANT Mobile Guardian	Mobile Guardian addresses mobile security issues with centrally managed security policy administration, device discovery and on-going policy enforcement. www.credant.com
IBM Tivoli Configuration Manager	Integrate server management with device management to minimize the TCO (total cost of ownership). Functionality includes inventory capture, software distribution, configuration management, automatic device profile recovery and mobile security support for servers, desktops and mobile devices. www.tivoli.com
iAnywhere Afaria	Afaria helps companies secure devices, automate processes and manage software, content and data. IT can define management and security policies from a central console and apply them to groups of users automatically. www.ianywhere.com
Intellisync Mobile Systems Management	Manage and secure mobile devices from a central console with Intellisync Mobile Systems Management. Functionality includes software distribution, asset collection, device configuration management, troubleshooting, backup and recovery. www.intellisync.com
Trust Digital TRUST Enterprise Secure	TRUST Enterprise Secure provides a policy-based framework to automate the creation, deployment, enforcement, auditing and control of security policies. www.trustdigital.com
Novell Zenworks Handheld Management	ZENworks simplifies the deployment, management and maintenance of IT resources in today's diverse environments. With Handheld Management, IT can centrally administer password policies, implement self-destruct or lockout capabilities, conduct centralized backups, and define and apply policies based on users groups of users or devices. www.novell.com

Transmission security solutions

PRODUCT	FEATURES
Aventail Workplace	SSL VPN technology delivers strong security using SSL, proxy protection from direct network access, and seamless integration with directories. www.aventail.com
F5 Firepass	F5 FirePass SSL VPN provides a Web-based method of extending secure remote access to mobile users - with no special software on the client and no modifications to back-end resources. www.f5.com
IBM WebSphere Everyplace Access (WEA)	WEA provides secure, wireless access to enterprise applications and data. Features include: PIM and email sync. www.ibm.com
Meetinghouse AEGIS WLAN Security Solution	AEGIS supports LEAP, an 802.1x standards-based authentication method developed by Cisco. LEAP requires mutual authentication, which means both the user and access point must authenticate one to the other before network access is granted. www.mtghouse.com
Certicom movianVPN	movianVPN is an IPSec VPN client that provides strong authentication, encryption and data integrity checking to secure remote access to email and data. movianVPN supports a wide variety of popular gateways, including Cisco, Lucent and Nortel. www.certicom.com
Mergic Mergic VPN	Mergic VPN is a PPTP (Point-to-Point Tunneling Protocol) VPN client for securing remote access. Mergic VPN works with many popular VPN servers from Cisco, Microsoft, Linux and Nortel. www.mergic.com
Nortel Networks Alteon SSL VPN	Alteon SSL VPN extends the reach of enterprise applications to mobile workers. By using secure sockets layer (SSL) as the underlying security protocol, Alteon SSL VPN uses the Internet for remote connectivity and the Web browser as the primary interface. www.nortel.com
WorldNet21 anthaVPN *(formerly movianVPN)*	anthaVPN, an IPSec-based VPN client, provides strong authentication, encryption and data integrity assurance for secure remote access to email and data. anthaVPN supports many popular gateways, including Cisco, Lucent and Nortel. www.anthavpn.com

Cryptography and PKI Toolkits

PRODUCT	FEATURES
Certicom Security Builder® Crypto™	Security Builder Crypto is optimized for small code size and includes a range of current and legacy algorithms that provide proven security. See GSE version above. www.certicom.com
Copera AESLib	AESLib is a shared library that implements the AES encryption algorithm. Version 3.1 includes ARM support. www.copera.com
Diversinet Passport	Passport client/server security software facilitates digital signatures, authentication and encryption with PKI products specifically optimized for wireless environments and devices. www.diversinet.com
RSA Security BSAFE	The RSA BSAFE line of SDKs provides all of the components required to make any application safe and secure, including web services security, protocol implementations, certificate management and cryptography. www.rsasecurity.com
Ntru Cryptosystems Security Toolkit	Ntru offers a full range of public and symmetric key functionality, including encryption, decryption, signing and verification. www.ntru.com

Anti-virus applications

PRODUCT	FEATURES
Computer Associates eTrust Antivirus	eTrust Antivirus detects viruses and Trojans that infect devices. www.ca.com
Symantec AntiVirus	Scans files automatically and prompts the user if malicious code is detected. In addition, AntiVirus can update virus definitions wirelessly or via synchronization. www.symantec.com

Messaging and data solutions

PRODUCT	FEATURES
Good Technology GoodLink	With GoodLink, users can exchange messages, access data, and manage phone calls from their Treo smartphone. www.good.com
Notify NotifyLink Enterprise Edition	NotifyLink Enterprise Edition Is designed for small to large-scale corporations requiring secure wireless push notification of email, calendar, contacts, and tasks, for their mobile professionals. NotifyLink supports multiple devices, multiple networks, global settings, and encryption of messages. www.notifycorp.com
Intellisync Mobile Suite	Intellisync Mobile Suite keeps mobile devices synchronized with Exchange and Domino groupware applications. Intellisync also provides IT with tools for management and support such as remote installation/upgrades, device configuration, backup/restore, and asset inventory collection. www.intellisync.com
SEVEN System SEVEN	System SEVEN is a mobile software architecture deployed at the operator network that provides access to email, calendar, contacts, documents and corporate directories. www.seven.com
Visto Mobile Access Solution	Visto Mobile Access Solution TM, Server Edition provides secure mobile, wireless access to Microsoft Exchange and Outlook data. www.visto.com
Extended Systems OneBridge Mobile Groupware	OneBridge enterprise synchronization software enables mobile workers to access and synchronize e-mail, PIM and custom database information. www.extendedsystems.com

Please contact the solution provider for the latest product features and platform support information.

Glossary

3DES or TDES: Triple DES, a stronger version of DES encryption in which the input data is, in effect, encrypted three times.

802.11: A family of specifications developed by the IEEE for wireless LAN technology. The most commonly deployed 802.11 specification is 802.11b, also called Wi-Fi.

802.1X: An IEEE standard based on the Extensible Authentication Protocol that provides an authentication framework for 802.11 LANs.

AES: Advanced Encryption Standard, FIPS 197. Originally named Rijndael, AES is a block cipher algorithm that was selected by NIST as the "Advanced Encryption Standard."

Algorithm: A specific mathematical formula to perform a function (like encryption and decryption). Some algorithms are more secure than others, while some are faster than others.

Asymmetric Encryption: Any encryption scheme where the sender and receiver use a pair of different but related keys that cannot be derived from one another. Data is encrypted with one of the keys and decrypted with the other key.

Biometric Authentication: Any method for verifying identity that relies on a unique personal attribute, such as fingerprint, voice or the blood vessel pattern around a retina.

Bluetooth SIG: Bluetooth Special Interest Group. The trade association of wireless company representatives and other experts who define and maintain the Bluetooth specification for short-range wireless transmission.

Blowfish: A symmetric block cipher developed by Bruce Schneider in 1993. Blowfish has undergone considerable review and is gaining acceptance as a strong encryption algorithm.

CDMA: Code Division Multiple Access

Certificate: A public key digitally signed by some signing authority to guarantee its validity.

Certificate Authority: A trusted third-party clearinghouse that issues digital certificates and digital signatures.

CHAP: Challenge Handshake Authentication Protocol. A type of authentication in which the authentication agent (typically the network server) sends the client program a key to be used to encrypt the username and password.

Checksum: A technique whereby the individual binary values of a string of data are totaled at two points in time to determine if any data has been changed. Commonly used to check the integrity of data that has been transmitted or stored.

Cipher: The generic term used to describe a means of encrypting data. "Cipher" may also refer to the encryption algorithm itself.

Encryption: Any method of scrambling data so that it cannot be read during storage or transmission. The data is then kept confidential until it is decrypted (unscrambled).

ESN: Electronic Serial Number

Flash ID: Unique serial number for the ROM in a Palm device.

GPRS: General Packet Radio Service

FIPS: Standards and guidelines for federal computer systems issued by NIST.

GSM: Global System for Mobile Communications

HIPPA: U.S. legislation that, among other things, sets standards for the security of protected health information.

HMAC: Hashed Message Authentication Code. A message digest function and secret key used to create authentication codes using MD5 or Secure Hash Algorithm (SHA).

HSN: Hardware Serial Number. A unique number or alphanumeric combination assigned to a device.

IEEE: Institute of Electrical and Electronics Engineers. A large, international, non-profit, technical professional association that establishes consensus-based open standards.

IETF: Internet Engineering Task Force. A large open international community of professionals concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

IMEA: International Mobile Equipment Identity

IPSec: Internet Protocol Security. A tunneling protocol developed by IETF and often used to implement VPN security.

IR port: Infrared Port. A port built into many models of smartphones and handhelds for transfer of data between devices.

ISO: International Organization for Standardization, a worldwide federation of national standards bodies from more than 140 countries.

ISP: Internet Service Provider.

Key: Typically an alphanumeric string used for encryption and/or decryption.

LDAP: Lightweight Directory Access Protocol. An open standard for directory lookups that uses a hierarchical structure.

LAN: Local Area Network. A network that encompasses a small physical area (e.g. one office).

MD5: A one-way hash algorithm used to create a message digest for digital signatures.

MMC: MultiMedia Card. A removable storage media that can be used in many electronic devices, including Palm handhelds and smartphones.

NIST: National Institute of Standards and Technology, a nonregulatory agency within the U.S. Commerce Department that develops and promotes measurements, standards, and technology.

PAN: Personal Area Network. A wireless network that enables handhelds, smartphones, cell phones, and other mobile devices to communicate over short distances.

PKI: Public Key Infrastructure. A system of digital certificates, Certificate Authorities, and other registration authorities used to verify and authenticate each party in a transaction.

PPP: Point-to-Point-Protocol

PPTP: Point-to-Point Tunneling Protocol. A protocol developed by Microsoft, commonly used for VPN security.

Public Key Encryption: An asymmetric encryption scheme such as RSA, Diffie-Hellman-Elgamal, and Elliptic Curve algorithms.

RADIUS: Remote Authentication Dial-In User Service. An authentication and accounting system used by many Internet service providers. The specification is maintained by IETF.

SAFER+: An encryption algorithm submitted by Cylink Corporation as an AES candidate. SAFER+ provides slightly less than the suggested 2128-order protection, given 128-bit keys, which is why it was not chosen for AES. Experts agree, however, that this academic imperfection does not compromise SAFER+ in practice.

SET: Secure Electronic Transaction. An open industry standard protocol developed for the secure transmission of payment information over the Internet and other electronic networks.

SD: Secure Digital card. A removable storage media that can be used in many electronic devices, including Palm handhelds and smartphones. SD uses the same form factor as MMC.

SDIO: Secure Digital Input/Output.

SHA-1: Secure Hash Algorithm. A popular algorithm for computing cryptographic checksums. Checksums are commonly used to check if data has been modified.

SSL: Secure Socket Layer. A very popular protocol for managing the security of message transmission over the Internet. SSL is found in virtually all commercial web browsers today.

Symmetric Encryption: Any encryption scheme where the encrypting and decrypting parties share the same key.

TKIP: Temporary Key Integrity Protocol. An interim fix to WEP encryption problems. TKIP can be applied to existing hardware through driver and firmware upgrades.

USB: Universal Serial Bus, a plug-and-play interface between a computer and add-on devices.

VPN: Virtual Private Network. A network which emulates a private network, although running over a public network. The use of encryption and a tunneling protocol maintains privacy.

WAN: Wide Area Network. A computer network that encompasses a wide physical area. Multiple LANs are often connected to form a WAN.

WEP: Wired Equivalent Privacy. A security protocol for wireless local area networks defined in the 802.11b specification.

Palm, Inc.
950 W Maude Ave
Sunnyvale, CA 94085-2801
www.palm.com

P 483 05